ChinaXiv合作期刊
知识管理论坛 ISSN 2095-5472 CN11-6036/C
Knowledge Management Forum
E-mail: kmf@mail.las.ac.cn
http://www.kmf.ac.cn

【学术探索】

大数据环境下智慧城市信息安全保障体系构建研究

邹凯[1] 郭一航[1] 向尚[2] 万震[1]
1. 湘潭大学公共管理学院 湘潭 411105
2. 国防科技大学系统工程学院 长沙 410073

摘要： [**目的 / 意义**] 大数据环境下智慧城市面临的信息安全问题日益突出，基于此构建大数据环境下全面感知、系统运作、协同整合的智慧城市信息安全保障体系，优化大数据环境下智慧城市信息安全管理，完善当下智慧城市信息安全建设具有一定的理论意义和实践价值。[**方法 / 过程**] 将全面质量管理理论应用到智慧城市信息安全保障体系研究中，立足于信息安全的四项基本内涵，借助 PDCA 循环的 4 个阶段构建大数据环境下智慧城市信息安全保障体系基本架构。[**结果 / 结论**] 通过 PDCA 循环解决智慧城市信息安全保障问题，符合城市建设和发展过程应不断动态调整的特点，为保障大数据环境下智慧城市信息安全的全过程实施提供参考，主要包括：规划阶段的"方向＋目标、规范＋约束、计划＋指标"，实施阶段的组织结构、基础设施和技术体系，控制阶段的态势感知、应急响应和风险管理，改进阶段政府、运营方和公众的多主体协同。

关键词： 智慧城市 大数据 信息安全 PDCA 循环 保障体系
分类号： G203

引用格式： 邹凯，郭一航，向尚，等．大数据环境下智慧城市信息安全保障体系构建研究 [J/OL]. 知识管理论坛，2021, 6(6): 364-374[引用日期]. http://www.kmf.ac.cn/p/268/.

1 引言

随着 Web2.0、物联网和云计算等技术的广泛使用，在智慧城市建设和运营过程中，政府、企业和社会之间的信息交换和信息共享日趋频繁，产生大量数据资源的同时也带来许多非传统性的信息安全问题，这些问题相互交织和叠加引发的隐私泄露事件呈指数增长，极易造成

基金项目： 本文系国家社会科学基金项目"大数据环境下智慧城市信息安全困境及应对策略研究"（项目编号：18BTQ055）研究成果之一。
作者简介： 邹凯，教授，博士；郭一航，硕士研究生，通信作者，E-mail：709069371@qq.com；向尚，博士研究生；万震，硕士研究生。
收稿日期：2021-09-02 发表日期：2021-11-30 本文责任编辑：刘远颖

知识管理论坛，2021（6）:364-374
DOI: 10.13266/j.issn.2095-5472.2021.034

不良的经济影响和社会影响。我国“十四五”规划纲要指出，要“在推动新一代信息技术同各产业深度融合的同时，保障国家数据安全，推动大数据中心建设”。大数据作为推动智慧城市快速发展的关键技术，将城市公共基础设施运行系统的各项关键信息进行整合，跟踪了解城市运行情况，统筹管理各方信息资源，监测处理各种突发状况，促进传统数据中心向高算例、高效能的新型数据中心演进，有利于保证城市运行的良好态势。

目前国内外学者对于智慧城市信息安全的相关研究成果较为丰富，沈明欢 [1] 首次提到应高度重视从战略层面加强对智慧城市信息安全的管理，Chen Z Y [2] 在对智慧城市进行可视化数据处理时首次提到信息安全的保护，在此背景下，国内外学者开始逐步展开对智慧城市信息安全的研究。在研究初期，多以定性和宏观层面的研究为主，对智慧城市信息安全的基本内涵 [3]、现状困境 [4-7]、风险评价 [8]、关键技术 [9]、保障策略 [10-11] 等进行探讨。随着研究的逐渐拓展，国内外学者开始尝试对智慧城市信息安全进行量化分析、创新性技术融合和具体实践应用的深入研究，对智慧城市信息安全风险管理中的风险预测 [12-13]、风险评估模型 [14-15]、风险要素识别 [16-17]、风险监管 [18] 等进行探讨，并从不同维度 [19]、不同层次 [20] 构建了智慧城市信息安全体系以应对智慧城市运营中的风险，有关学者在此基础上对其做出了进一步的完善 [21-22]。对新一代信息技术 [23-26] 在智慧城市建设的深度融合进行研究，并探究相关技术在不同智慧应用场景中实现安全隐私保护的具体实践 [27]。

综上所述，国内外学者在智慧城市信息安全许多方面的研究较为成熟，在保障体系方面，虽有少量研究成果，但缺乏系统性的规划和成熟的理论指导，特别是在大数据环境下，信息安全中的数据正呈现一种多维融合、多利益主体开放共享、万物跨域互联、软硬件重叠渗透、协同和整合中汇聚的全新形态，这大大增加了信息安全管理的复杂性、交织性、动态性和综合性 [28]。信息安全不单单只是技术问题，而是各方面的协同管理问题 [29]，因此，构建完善的智慧城市信息安全保障体系是当务之急。笔者从顶层设计的角度，首先分析大数据环境下智慧城市信息安全面临的挑战和智慧城市信息安全基本内涵之间的内在联系，其次基于全面质量管理理论的 PDCA 循环，对智慧城市信息安全工作的不同阶段实施全方位的动态质量管理，最后构建注重业务需求、持续改进的信息安全保障体系，满足智慧城市信息安全建设需要，以期为智慧城市信息安全保障的具体实践献言建策。

2 大数据环境下智慧城市信息安全保障体系的形成

2.1 大数据环境下智慧城市信息安全面临的挑战

智慧城市的建设与大数据技术的发展应用，开启了大规模实时、在线、多方协作的社会治理的新局面。借助大数据，可以为城市的规划、管理、安防与防灾、舆情监控等领域提供强大的决策，以达到优化行政资源、降低管理成本、提高管理效率和应急响应能力的目标。大数据技术在驱动城市智慧升级的同时，也带来更加严峻的信息安全挑战，主要包括 3 个方面：①传统防护方式变得复杂和困难。在大数据环境下，传统的数据隔离、数据加密、访问控制、容灾备份等数据防护方式需要进一步革新。在数据的传输、处理及存储的各个环节中，存在着不同以往的数据泄露、篡改与破坏的风险。②数据融合和共享导致管理工作复杂化。数据的高度融合与开发给信息安全管理带来了空前的挑战。宏观上，智慧城市的信息安全保障体系、相关配套法律法规和监督管理机制尚不健全，防护手段能力建设仍处于起步阶段；微观上，针对智慧城市不同信息系统之间的运行环境、系统架构、数据库系统、数据格式等，信息安全工作者需要设计不同的安全策略和防控方案，运营管理和监控审计难度也进一步加大。③个人的隐私保护和数据安全变得更加紧迫。大数

据时代信息即价值的理念深入人心，有关企业在收集大量非必要的个人信息后进行擅自披露和传播，加剧了个人信息的滥用，更有甚者通过售卖个人信息获取不正当利益的行为也屡见不鲜，如在“315”晚会上曝光的“人脸信息非法盗用”和“简历平台个人信息非法售卖”等事件加剧了人们对大数据时代信息安全的担忧，“滴滴平台因信息外露下架”事件更是威胁到了国家安全。此外网络黑客利用企业存在的技术漏洞、监管不力等因素多方位盗取个人信息和数据，进而实施电信诈骗等违法犯罪行为。在如今的泛在网络时代下，不法分子可以通过大数据分析技术动用较少的资源实现多维度、共时性的网络攻击，其造成的信息安全威胁更加精准并更具危害性。

2.2 大数据环境下智慧城市信息安全基本内涵

结合国家《计算机信息系统安全保护条例》，可以将智慧城市信息安全的基本内涵分为物理安全、数据安全、运行安全和管理安全 4 个方面：物理安全是指通过智慧城市信息系统实体有关的硬件设施与环境建设而进行的物理安全设计，构筑出安全的物理网络。数据安全是为数据处理系统建立的安全保护，确保网络数据的可用性、完整性和保密性。运行安全是着眼于智慧城市运行工作特点，利用安全技术与措施保护信息处理、分析与使用过程中的安全。管理安全是通过制定相应标准规范和制度规则，对智慧城市信息安全工作人员的日常工作和行为进行管理和约束。对上述 4 个方面进行全方位动态管理有利于应对大数据环境下智慧城市信息安全带来的巨大挑战。

2.3 大数据环境下智慧城市信息安全保障体系架构

全面质量管理理论于 20 世纪 50 年代末由美国通用电气公司的费根堡姆和质量管理专家朱兰提出，它是一种实现预先控制和全面控制的管理制度，达到对象、过程、人员、范围的全面管理。戴明博士将全面质量管理的工作程序总结为“计划（plan）—实施（do）—检查（check）—处理（act）”四阶段的循环方式，简称戴明环（PDCA），它是一个周而复始、大环套小环、小环推动大环、阶梯性上升的循环体系 [30]。目前，在信息安全方面，戴明环（PDCA）在不同行业 [31-33]、不同组织 [34-36] 中都有广泛研究和应用。智慧城市信息安全建设是以信息安全保障质量为中心，以政府、企业和公众的参与为基础，达到全员收益并获得成功的长期工程。笔者在借鉴 ISO/IEC 27001：2005 标准的基础上，进行大数据环境下智慧城市信息安全保障体系的构建，如图 1 所示：

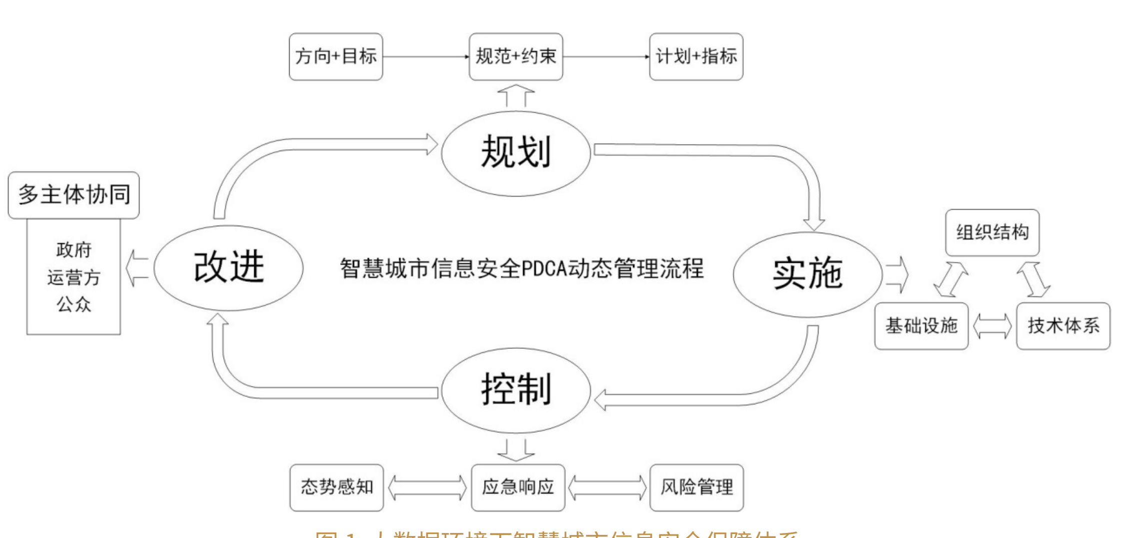


图 1 大数据环境下智慧城市信息安全保障体系

知识管理论坛，2021（6）:364-374
DOI: 10.13266/j.issn.2095-5472.2021.034

笔者通过借鉴PDCA模式循环控制的思想，将智慧城市信息安全保障体系分为“规划—实施—控制—改进”4个阶段。在规划阶段，依据智慧城市信息安全保障战略规划特征，确立整体目标；在实施阶段，根据全面质量管理的“结构、技术、人员、变革推动者”4个基本要素，将智慧城市的信息安全实施过程分为组织结构、基础设施、技术体系三部分，保障智慧城市的物理安全和数据安全；在控制阶段，依据大数据环境下智慧城市信息安全特点，结合国家标准GB/T 20282-2006《信息安全技术信息系统安全工程管理要求》，从态势感知、应急响应、风险管理3个方面对数据运营及业务流程进行有力管控，保障智慧城市的运行安全和管理安全；在改进阶段，针对国家角度、智慧城市服务方角度、公众角度对智慧城市信息安全提出不同的改进要求和建议，形成智慧城市信息安全保障体系完整架构。

3 大数据环境下智慧城市信息安全保障全过程

3.1 大数据环境下智慧城市信息安全保障的规划阶段

智慧城市信息安全规划的首要工作是确定整体方向和宏观目标，政府在收集社会公众和各方组织的建议之后，借助大数据分析及挖掘技术和信息安全防护特点，确定信息安全工作的建设目标，为信息安全实施、控制过程提供指导性意见，指导信息安全工作的开展。其次，政府要在顶层框架下规划管理风险的基本要素建设，同时协调机会、环境与各方组织资源之间的平衡，在《数据安全法》和2021年11月1日刚刚施行的《个人信息保护法》等法律法规和相应的方针政策指导下，规范和约束信息安全组织的活动和工作。最后，信息安全主管部门要制定对应的详细计划和指标，设计质量评估模型，开发数据质量技术，加强管理规章制度建设和管理手段建设，落实安全管理措施。如相关云服务以及供应链提供商要签订信息安全保证书，在公司内部形成切实有效的信息安全保障计划和考察指标，严格遵照国家标准和行业规范进行管理和运作。

3.2 大数据环境下智慧城市信息安全保障的实施阶段

在智慧城市信息安全实施过程中，根据全面质量管理的“结构、技术、人员、变革推动者”4个基本要素，将智慧城市的信息安全实施过程分为组织结构、基础设施、技术体系3个部分，保障智慧城市的物理安全和数据安全。

3.2.1 智慧城市信息安全组织结构建立

在智慧城市信息安全保障实施阶段，为了实现不同应用项目的信息安全建设，需要建立专业化、部门化和正规化的信息安全组织结构，协调各级、各类信息组织的分工、分组和协调合作。智慧城市信息安全组织结构建设要根据智慧城市信息系统的目标和工作计划，将各项资源按照一定的规则联结成为相应的模块，设立不同层次的业务与行政部门，并规定部门内部的人员编制和职权分工，以及相互之间的隶属关系，使智慧城市信息安全组织成为一个结构有序合理、功能完备的有机整体。结合智慧城市信息安全具体实践的特点，从智慧城市信息安全的实际需求出发，建立智慧城市信息安全组织的“金字塔”结构，如图2所示。

信息安全领导小组是智慧城市信息安全决策机构，主要是从全局的角度确定信息安全工作的战略和方向，部署信息安全管理工作，对智慧城市信息安全项目进行有效控制。

信息安全监督机构是监督信息安全管理委员会和执行机构的相关工作，并将审查结果汇报给智慧城市信息安全领导小组，为各部门和各业务系统的信息安全工作提供改进意见。

信息安全管理委员会通过提供信息为决策机构提供决策支持，制定信息安全工作的相关规则，对信息安全项目进行评审和质量控制，管理信息安全执行机构，并定期向智慧城市信息安全监督机构汇报信息安全情况。

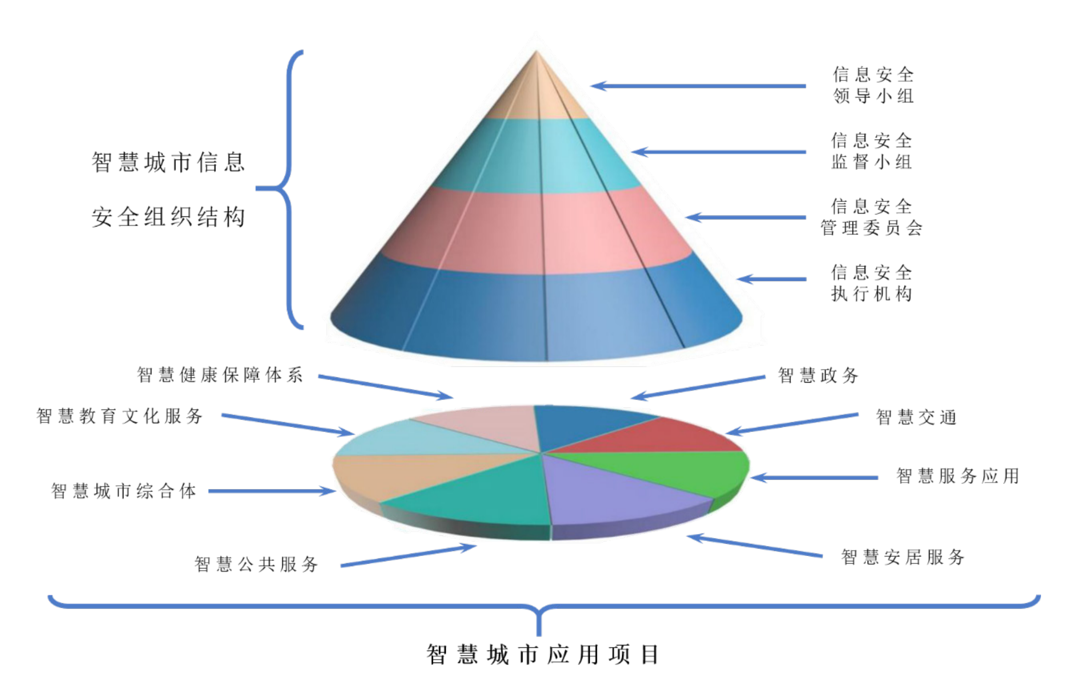


图 2 智慧城市信息安全组织结构

信息安全执行机构包括信息安全运维团队和信息安全事件响应小组，负责贯彻和落实上级部门的信息安全方针政策以及各项工作要求，及时响应和处理智慧公共服务、智慧城市综合体等八大应用项目内的信息安全突发事件 [37]。

3.2.2 智慧城市信息安全基础设施建设

智慧城市信息安全基础设施建设是智慧城市信息安全保障的物质基础。通过信息安全基础设施建设可以实现信息安全数据共享、信息内容监控、有害信息过滤等，有利于智慧城市相关应用项目的网络安全保障与空间治理。国脉互联 [38] 将智慧城市的基础设施分为 3 个部分，如表 1 所示：

表 1 智慧城市信息安全基础设施

信息安全基础设施分类	信息安全基础设施内容
信息网络设施	有线宽带、无线宽带 城市物联网、三网融合等
信息共享设施	云计算平台 信息安全服务平台 测试中心等
智能化传统设施	水、电、气、热管网 道路、桥梁、车站、机场等

结合国务院最新公布的《关键信息基础设施安全保护条例》，智慧城市信息安全基础设施建设的推进工作应主要包括 3 个方面：①要统筹安排信息安全基础设施的建设工作，对智慧城市信息安全进行全盘管理与系统规划，规定工作中获取的信息只能用于维护网络安全；②要紧密跟踪和研究国外的发展趋势和技术进展，结合大数据环境下智慧城市信息安全技术特点提升基础设施能力，如升级基础设施、扩大带宽、改进入侵检测技术等；③要加强各网络指挥中心的沟通与连接，融合各单位的工作能力，通过协调分析等手段加强智慧城市信息安全在线监测和态势感知方面的合作，建立网络安全信息共享机制。

3.2.3 智慧城市信息安全技术体系构建

信息安全技术核心目标一般包括保密性、完整性、可用性、可控性和不可否认性等，遵照信息安全的安全隔离、动态保护和深度保护等原则，从层次、空间、等级 3 个维度建立相对全面、完整的智慧城市信息安全技术体系，如图 3 所示：

知识管理论坛，2021（6）:364-374
DOI: 10.13266/j.issn.2095-5472.2021.034

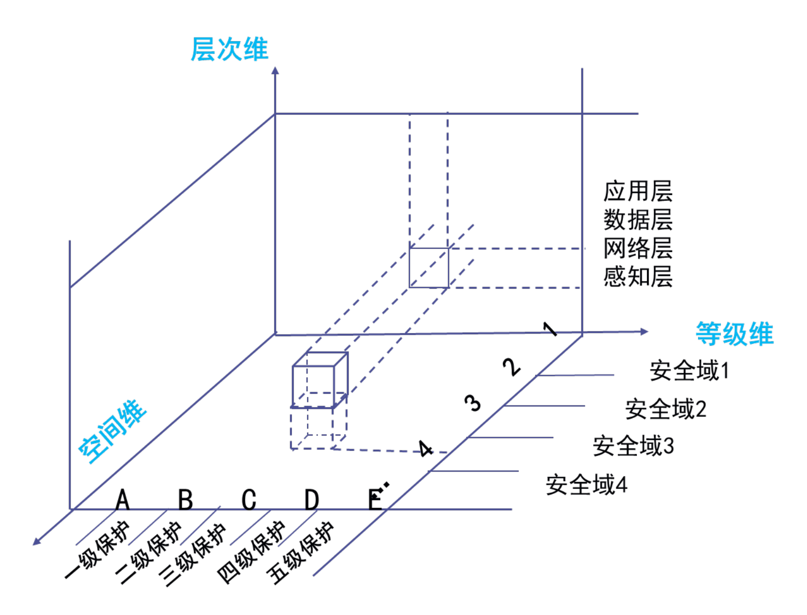


图 3 智慧城市信息安全技术体系

在层次维中，智慧城市各个信息系统通过对计算机硬件、软件、网络和通信设备等基础设施进行集成，处理智慧城市内部业务的各项信息流，可以分为感知层、网络层、数据层和应用层 [39]4 个方面。智慧城市信息系统的 4 个层次层层递进，底层设施的安全缺失影响到高层的运行安全，形成信息安全威胁上下交织，从而影响整个系统的安全性。在信息安全环境搭建过程中，对信息安全产品逐层构建，同时注意各层次信息安全产品间的兼容和互补关系，避免安全策略和安全因素之间的矛盾。

在空间维中，通过网络连接成无数个大小各异的分布式网络系统，针对不同网络区域内的安全性目标，其保护策略和技术手段也会有一定的差异，需要依据不同区域的特点采用分域保护的措施。对现有的计算机网络系统构成和信息安全工程的具体实践进行系统分析和总结，可以将智慧城市的网络信息系统分为局域计算环境、网络边界、网络传输和网络基础设施 4 种类型 [40]，在各区域使用身份验证、物理隔离、入侵检测等安全技术和相关安全产品，保障各安全域内的信息安全。

在等级维中，智慧城市不同应用项目和业务部门对信息安全的要求和重要程度是不同的，对于信息安全保护所付出的成本和代价也会不同，因此结合《数据安全法》中对数据实行分类分级保护的思想，将智慧城市信息安全保护分为 5 个等级 [41]。对关系到智慧城市建设和运营的关键信息和城市居民隐私实施重点保护，对次要信息给予适当保护。另外，在智慧城市信息安全技术体系的构建过程中，要根据信息安全理论与方法的不断完善和技术的不断提升，同步加强信息系统各个方面的防范与保护。

3.3 大数据环境下智慧城市信息安全保障的控制阶段

在智慧城市信息安全控制过程中，依据大数据环境下智慧城市信息安全特点，在智慧城市信息安全基本要素建立的基础上，结合国家标准 GB/T 20282-2006《信息安全技术信息系统安全工程管理要求》，从态势感知、应急响应、风险管理 3 个方面对数据运营及业务流程进行有力管控，保障智慧城市的运行安全和管理安全。

3.3.1 智慧城市信息安全态势感知

智慧城市信息安全态势感知的重点是保护城市网络环境中核心应用的安全稳定以及持续

运行，通过标识和报告智慧城市建设和运营中所有信息安全违规行为，对有关事件进行探测和追踪，并根据安全目标和安全策略处理城市信息安全态势变化。城市网络核心应用涉及智慧城市应用项目内部各项资产的监管问题，因此态势感知需要紧紧围绕“资产—数据—态势”这一主线，针对资产的结构、管理、服务状态等方面可能产生的安全威胁进行识别分析和响应处理。

在资产层中，资产信息和监控数据在经过数据规约、数据融合等预处理之后，利用相应的资产数据库、事件数据库等进行表示和存储，为数据层提供相应的数据支持。在数据层中，通过应用大数据环境下网络特征提取技术、与关联分析技术等相关智能算法与安全模型，将存储的数据进行深度挖掘处理，标识出影响智慧城市信息系统运行态势的安全事件。在态势层中，应在安全事件处理过程中根据实时的数据反馈，依据数据可视化技术监督系统安全态势变化，预测系统安全状况和安全事件的发展趋势，做出前瞻性判断，提前预警信息安全相关威胁。

3.3.2 智慧城市信息安全应急响应

智慧城市信息安全应急响应是为应对智慧城市系统中各种信息安全事件的发生，而在事发前所做的准备工作和在事后所采取的紧急措施 [42]。智慧城市信息安全应急响应可以分为应急准备、事件预警、应急处理和事件评估4个部分。由于信息安全事件处理的及时性和有效性特点，事件预警与应急处理往往是相伴而生，同时进行的。而事件评估则是贯穿应急响应的整个过程，对智慧城市信息安全应急响应过程、各类机构以及人员行为等进行测评和管理。

在应急准备中，信息安全管理机构参照《信息安全事件分类分级指南》，按照信息系统的重要程度、系统损失和社会影响3个考虑因素，划分事件的不同类别和级别，并制定相应的信息安全应急预案，在安全事件发生时采取有效预案，快速做出响应。

在事件预警和应急处理中，当智慧城市业务系统中发生信息安全事件时，如果安全事件处于控制之下，信息安全执行机构立即启用对应信息安全预案做出响应，做好充足的信息准备，记录所有活动以供后续评审之用。反之，如果安全事件不处于控制之下，应及时发出事件预警，按要求填写信息安全事态和事件报告单，上报给信息安全事件响应小组ISIRT(Information Security Incident Response Team ）。此外，如果判断事件属于重大信息安全事件，应立即报告给ISIRT管理者和高级管理层。

在事件评估中，信息安全管理委员会和信息安全监督机构应收集和安全保存事件应急过程中的相关电子证据，为后续法律起诉或者内部人员奖惩提供支持。在安全事件解决后，信息安全管理委员会根据报告中详细应急记录进行事件评估，从安全事件及其防护措施中吸取经验和教训，必要时修改已有的应急预案，防范类似安全事件再次发生。

3.3.3 智慧城市信息安全风险管理

智慧城市在运行过程中由于其软硬件系统的多样化、系统集成和网络连接中必然会存在缺陷和潜在的薄弱环节，因此会引发不同程度的信息安全风险。参照前人 [43-46] 的研究基础，笔者认为对于智慧城市信息安全风险管理应该采用目标驱动的管理模式，进行智慧城市信息安全风险管理建模，并加强风险库的建设，如图4所示。

首先，通过大数据采集技术获取海量信息安全原始数据，分析智慧城市内部业务需求特点，设定业务需求的信息安全控制点，对流程的重要边界进行定义，确定智慧城市信息安全风险管理的目标，完成目标驱动下的风险管理准备工作。

其次，针对信息系统的业务目标和安全需求，建立相应风险管理业务流程。开展智慧城市信息安全风险管理工作时，通过分析与识别系统中各类数据特征和安全属性，确定资产、威胁、脆弱性和控制措施列表。对

知识管理论坛，2021（6）:364-374
DOI: 10.13266/j.issn.2095-5472.2021.034

于智慧城市信息系统中各类已知风险，从风险模型库中选取大数据环境下相应的智能算法与数学模型，分析信息安全风险威胁指数，划分风险相应等级，预测风险发生的可能性和造成的社会影响，并将提取的信息安全风险模式和相关特征数据存储到风险数据库中。根据得到的风险模式和特征数据，从风险知识库中获取处理此类风险的制度、技术和管理上的相关规则及应对措施，并对风险解决结果进行评估审核、存储备案。

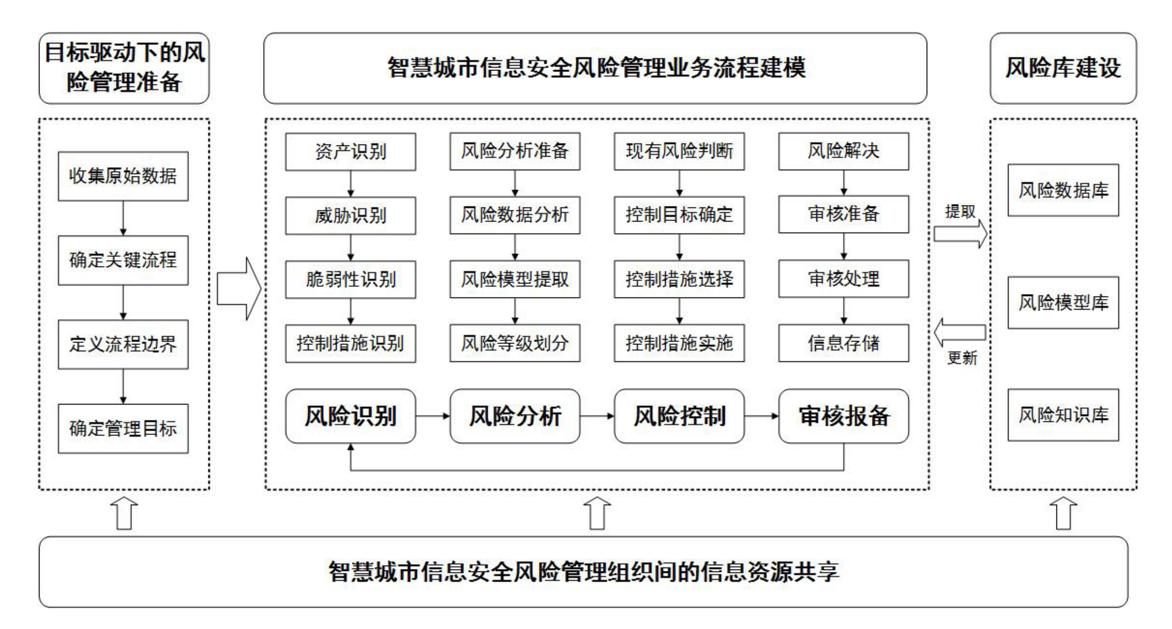


图 4 大数据环境下智慧城市信息安全风险管理流程

最后，针对发现的新型信息安全风险或者已有风险的新变化，及时更新风险数据库、风险模型库和风险知识库。在处理信息安全风险时，要注意不同管理组织间的信息资源共享，协调各项组织的信息安全需求和工作任务。

3.4 大数据环境下智慧城市信息安全保障的改进阶段

大数据环境下智慧城市信息安全保障的改进是建立在规划、实施和控制之上的重要模块。通过 PDCA 循环的方式，能够推动大数据环境下智慧城市信息安全保障的问题解决和促进保障能力的不断提升。在改进阶段，涉及多元主体的共同参与，针对不同主体层次间的业务需求对智慧城市信息安全提出相应的改进要求。

立足国家宏观领导，整合各方资源。在智慧城市规划过程中，通过大数据技术全方位分析信息安全事件，在保证大方向的统一之下进行局部的目标调整和部署新的工作计划，推动智慧城市信息安全的组织结构、基础设施和技术体系的优化提升。在发挥自身领导优势的同时，借助大数据管理技术引导决策，平衡多方利益，整合各方资源，从传统低效的人工行政型政府转变为创新高效的数据服务型政府。

加大技术投入力度，推动空间治理。在智慧城市建设过程中，智慧城市信息基础设施以及服务提供商应加快在大数据环境下信息安全技术的开发与应用，利用大数据感知技术保护智慧城市关键网络应用，积极推进基于大数据的实时监督。同时，在完善大数据与云计算融合的新一代信息安全防护技术过程中，建立由态势感知、资产探测、运营中心等多套系统组成的网络空间普查工具，不断提升基于机器学习的云端安全防护技术。

促进社会公众参与，树立安全意识。在智

慧城市运营过程中，智慧城市治理领域不断呈现出主体多元化和参与深层化的特点，这就要求越来越多的社会公众参与到智慧城市治理工作中去。智慧城市中的信息通信技术能够随时随地地传播公众信息，保障智慧城市信息交流和意见反馈渠道的高效与畅通，实现市民对城市治理的电子参与（e-participation）。此外，要对市民在智慧城市信息安全建设的电子参与过程中产生的海量数据进行存储和深度挖掘，为智慧城市信息安全保障的规划提供改进建议。

4 结束语

笔者分析了大数据环境下智慧城市信息安全所面临的严峻挑战，结合智慧城市信息安全的基本内涵，将全面质量管理理论应用到智慧城市信息安全保障研究中，借助戴明环（PDCA）的 4 个阶段构建了大数据环境下智慧城市信息安全保障体系，以期为智慧城市信息安全管理研究和相关工作的开展提供借鉴思路和参考意见。本文虽然在理论层面有一定的创新性尝试，但由于各个城市的自身条件、特色和资源有所不同，在考虑智慧城市信息安全保障体系的构建时不可千篇一律，应考虑到具体城市信息安全建设的重点方向、应用规划与设计需求，在实际运用中仍需要做进一步探索和验证。智慧城市的建设和运营处于动态发展的进程之中，是一项规模宏大、内容全面、涉及多元主体的系统工程，因此智慧城市信息安全保障体系应结合城市建设和发展的动态过程不断调整。大数据技术为智慧城市信息安全的保障提供了一种新的解决方式，未来应加快大数据关键技术与智慧城市信息安全保障的进一步深度融合，推进大数据时代的信息安全管理范式变革和智能化决策体系的建立，促进智慧城市的持续健康发展。

参考文献：

[1] 沈明欢 .“智慧城市”助力我国城市发展模式转型 [J]. 城市观察 , 2010(3): 140-146.

[2] CHEN Z Y, FAN W, XIONG Z, et al.Visual data security and management for smart cities[J]. Frontiers of computer science in China, 2010, 4(3): 386-393.

[3] 李勇 . 智慧城市建设对城市信息安全的强化与冲击分析 [J]. 图书情报工作 , 2012, 56(6): 20-24.

[4] 邓贤峰 .“智慧城市”建设的风险分析 [J]. 财经界 , 2011(1): 106-109.

[5] ELMAGHRABY A S, LOSAVIO M M . Cyber security challenges in smart cities: safety, security and privacy[J]. Journal of advanced research, 2014, 5(4): 491-497.

[6] ZHANG K, NI J B, YANG K, et al. Security and privacy in smart city applications: challenges and solutions[J]. IEEE communications magazine, 2017, 55(1): 122-129.

[7] ALDAIRI A, TAWALBEH L. Cyber security attacks on smart cities and associated mobile technologies[J]. Procedia computer science, 2017, 109(3): 1086-1091.

[8] ABBAS H, MAGNUSSON C, YNGSTROM L, et al. Addressing dynamic issues in information security management[J]. Information management & computer security, 2011, 19(1): 5-24.

[9] 芦效峰 , 李海俊 . 智慧城市的支撑技术 —— 信息安全技术 [J]. 智能建筑与城市信息 , 2013(2): 90-98.

[10] FERRAZ F S, FERRAZ C. Smart city security issues: depicting information security issues in the role of an urban environment[C]// IEEE /ACM 7th International Conference on Utility and Cloud Computing, London：IEEE, 2014: 842-847.

[11] 宋璟 , 李斌 , 班晓芳 , 等 . 关于我国智慧城市信息安全的现状与思考 [J]. 中国信息安全 , 2016(2): 107-111.

[12] 向尚 , 邹凯 , 蒋知义 , 等 . 基于随机森林的智慧城市信息安全风险预测 [J]. 中国管理科学 , 2016, 24(S1): 266-270.

[13] QI L , HU C , ZHANG X , et al. Privacy-aware data fusion and prediction with spatial-temporal context for smart city industrial environment[J]. IEEE transactions on industrial informatics, 2020, 17(6): 1.

[14] 邹凯 , 向尚 , 张中青扬 , 等 . 智慧城市信息安全风险评估模型构建与实证研究 [J]. 图书情报工作 , 2016, 60(7): 19-24.

[15] 毛子骏 , 梅宏 , 肖一鸣 , 等 . 基于贝叶斯网络的智慧城市信息安全风险评估研究 [J]. 现代情报 , 2020, 40(5): 19-26, 40.

[16] 毛子骏 , 黄膺旭 , 徐晓林 . 信息生态视角下智慧城市信息安全风险分析及应对策略研究 [J]. 中国行政管理 , 2019(9): 123-129.

[17] 张艳丰 , 王羽西 , 邹凯 , 等 . 基于模糊 DANP 的智慧城

知识管理论坛，2021（6）:364-374
DOI：10.13266/j.issn.2095-5472.2021.034

市信息安全风险要素识别与管理策略研究 [J]. 情报理论与实践 , 2020, 43(10): 144-150.

[18] 邹凯 , 万震 , 曹丹 , 等 . 智慧城市信息安全监管策略的演化博弈分析 [J]. 现代情报 , 2021, 41(3): 3-14.

[19] 李洋 , 谢晴 , 邱菁萍 , 等 . 智慧城市信息安全保障体系研究 [J]. 信息技术与网络安全 , 2018, 37(7): 18-21.

[20] 张大江 , 毕晓宇 , 吕欣 , 等 . 智慧城市信息安全体系研究 [J]. 信息安全研究 , 2017, 3(8): 710-717.

[21] 王青娥 , 柴玄玄 , 张譞 . 智慧城市信息安全风险及保障体系构建 [J]. 科技进步与对策 , 2018, 35(24): 20-23.

[22] 杨天开 , 鲁洁 . 新型智慧城市环境下信息安全体系架构浅析 [J]. 中国管理信息化 , 2019, 22(19): 140-142.

[23] DAGHER G G , MOHLER J , MILOJKOVIC M , et al. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology[J]. Sustainable cities & society, 2018, 39(2): 283-297.

[24] MEMOS V A, PSANNIS K E, ISHIBASHI Y, et al. An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework[J]. Future generation computer systems, 2018, 83(6): 619-628

[25] WAZID M, DAS A K, VIVEKANANDA B K , et al. LAM-CIoT: lightweight authentication mechanism in cloud-based IoT environment[J]. Journal of network and computer applications, 2020, 150(1): 102496

[26] ULLAH Z, Al-TURJMAN F, MOSTARDA L, et al. Applications of artificial intelligence and machine learning in smart cities[J]. Computer communications, 2020, 154(3): 313-323.

[27] ZHANG K, NI J B, YANG K, et al. Security and privacy in smart city applications: challenges and solutions[J]. IEEE communications magazine: articles, news, and events of interest to communications engineers, 2017, 55 (1) : 122-129.

[28] 王世伟 . 论大数据时代信息安全的新特点与新要求 [J]. 图书情报工作 , 2016, 60(6): 5-14.

[29] 郭骅 , 苏新宁 . 智慧城市信息安全管理的环境、挑战与模式研究 [J]. 图书情报工作 , 2016, 60(19): 49-58.

[30] 黄水清 . 数字图书馆信息安全管理的过程方法 [J]. 图书情报工作 , 2013, 57(11): 5-11.

[31] 赵海 , 陈芳 . 电子支付信息安全管理体系的研究与实践 [J]. 信息安全研究 , 2019, 5(6): 534-541.

[32] 刘珊 , 杨华 , 岳克明 . 大数据在电力信息安全的研究 [J]. 山西电力 , 2018(4): 45-47.

[33] 吴璇 .PDCA 在医院信息系统安全监管中的应用 [J]. 网络安全技术与应用 , 2018(3): 114-115.

[34] 曾剑秋 , 程广焕 , 杨荫柯 . 电信运营企业信息安全风险管理体系研究 [J]. 科技管理研究 , 2016, 36(18): 160-164.

[35] 胡昌平 , 万莉 . 云环境下国家学术信息资源安全全面保障体系构建 [J]. 情报杂志 , 2017, 36(5): 124-128.

[36] 高东怀 , 沈霞娟 , 宁玉文 , 等 . 高校信息化管理服务体系研究 —— 以第四军医大学的实践为例 [J]. 武汉大学学报 (理学版), 2012, 58(S1): 65-69.

[37] 胡鑫 . 智慧城市 [J]. 电信技术 , 2016(9): 46-47, 51.

[38] 姜德峰 , 齐瑞瑞 . 智慧城市基础设施建设与评估 [J]. 电视技术 , 2013(14): 4-5.

[39] 范渊 . 大数据时代的智慧城市与信息安全 [M]. 北京 : 电子工业出版社 , 2018: 96.

[40] 王斌君 , 吉增瑞 . 信息安全技术体系研究 [J]. 计算机应用 , 2009, 29(S1): 59-62.

[41] GB/T 22240-2020, 网络安全保护等级定级指南 [S]. 北京 , 国家标准化管理委员会 , 2020.

[42] 王翔 . 网络与信息安全事件应急响应体系层次结构与联动研究 [J]. 网络安全技术与应用 , 2015(5): 177, 179.

[43] 曾志廉 , 黄丹凤 . 信息安全风险评估综合管理系统设计 [J]. 教育教学论坛 , 2016(23): 249-250.

[44] 武彬 , 张玉清 , 毛剑 . 信息安全风险管理系统的设计与实现 [J]. 计算机工程 , 2007(21): 134-136, 139.

[45] 官海滨 , 谢宗晓 , 王兴起 . 基于知识库的信息安全风险评估方法 Crisk 及其工具实现 [J]. 青岛大学学报 (自然科学版), 2013, 26(1): 66-70.

[46] 王桢珍 , 谢永强 , 武晓悦 , 等 . 信息安全风险管理研究 [J]. 信息安全与通信保密 , 2007(8): 162-164, 167.

作者贡献说明：

邹　凯：提出研究思路，起草与修订论文；
郭一航：设计研究框架，起草与修订论文；
向　尚：起草与修订论文；
万　震：收集相关文献，修订论文。


知识管理论坛
2021 年 第 6 期（总第 36 期）

Research on the Construction of Smart City Information Security Assurance System under the Big Data Environment

Zou Kai[1] Guo Yihang[1] Xiang Shang[2] Wan Zhen[1]

[1]School of Public Administration, Xiangtan University, Xiangtan 411105

[2]College of Systems Engineering, National University of Defense Technology University, Changsha 410073

Abstract: [Purpose/significance] The information security problems faced by smart cities under the big data environment are becoming more and more prominent. Based on this, building an information security assurance system of smart cities with comprehensive perception, system operation and collaborative integration under the big data environment, optimizing information security management of smart cities under the big data environment and perfecting the current information security construction of smart cities have certain theoretical significance and practical value. **[Method/process]** Applying total quality management theory to the research of smart city information security assurance system, based on the four basic connotations of information security, this paper built the basic structure of smart city information security assurance system under the big data environment with the help of the four phases of the PDCA cycle. **[Result/conclusion]** This research solves the problem of smart city information security through the PDCA cycle, which is in line with the characteristics of continuous dynamic adjustments in the process of urban construction and development, and provides references for the entire process of ensuring smart city information security under the big data environment. It mainly includes: in the planning stage, "directions + goals, norms + constraints, plans + indicators"; in the implementation phase, the organizational structure, infrastructure and technical system; in the control phase, situational awareness, emergency response and risk management; and in the improvement phase , the multi-agent coordination of the government, operators and the public.

Keywords: smart city big data information security PDCA cycle security system